Participatory Sensing or Sensing of Participation: Privacy Issues with Smartphone Apps Usage

Completed Research

Minoo Modaresnezhad
Information Systems and Supply Chain Management
University of North Carolina at Greensboro
m_modare@uncg.edu

Hamid R. Nemati
Information Systems and Supply Chain Management
University of North Carolina at Greensboro
nemati@uncg.edu

ABSTRACT

The convenience and mobility provided by smartphones have made them a preferred mode of conducting many daily activities and various types of applications for these devices have been developed. Apps on a smartphone can be used as a medium for tracking users' behaviors and collecting personal data about them. The collected data can potentially violate users' privacy. Many users may acknowledge this but their actions do not support that claim. The seeming inconsistency between professed privacy concerns and the use of smartphone apps may be more a consequence of ignorance rather than irrationality. In this study, an experiment is developed to understand how awareness about the privacy risks associated with the use of smartphone apps would alter the level of the use of apps. Our empirical results support the assertions that awareness significantly increases privacy concerns and reduces inclination to use apps. Implications of these findings are discussed.

Key Words
Privacy, participatory sensing, smartphone applications, ignorance.

INTRODUCTION

Communication has now gone digital and mobile, revolutionizing the way we communicate and socially interact with each other at work, school, gather information and entertain ourselves. The communication technologies that are currently most significantly impacting our lives are what collectively referred to as "smart devices" (such as smartphone, iPod/mp3, or tablet). Smart devices have become basic necessities. Perhaps the most dominate smart device in the market currently is the ubiquitous smartphone and is the focus of data collection for the present study. The convenience and mobility that smartphones provide have made them a preferred mode of conducting many of the daily activities previously requiring a computer, a trip to a store, a bank or a favorite entertainment establishment. They make life simpler by providing access to various products and services around the world at the touch of a finger. They bring the world into the user's palm. As a result, the use of these phones has skyrocketed. Companies have taken notice of this and have started developing various types of applications, henceforth referred to simply as "apps", for these devices at an increasing rate. Most users believe it is the apps that make the phone unique and not the phone's features or the phone's platform (Android, iOS, BlackberryOS etc.). Free and paid apps are being developed to provide users with various categories such as entertainment, news, navigation, shopping, medical etc.

However, smartphones are being termed as a "*boon in disguise*" by information security and privacy specialists since many of these apps, when downloaded and installed are used as a medium for tracking users' behaviors and collecting various personal data about them. While the collected data can be used for personalization, or providing preferential service, they can also be used for nefarious purposes thus violating privacy of users. Since these apps collect personally identifiable data at a very granular level, privacy issues are becoming a major area of concern. Though the apps provide users with comfort of accessing information, they are considered as a major threat to user privacy. Most of the mobile applications do not advertise or educate the users that their personal information are

being collected, stored, and processed without their knowledge and consent. Studies have shown that fear and distrust regarding the loss of personal privacy associated with the emerging technologies has been identified as one of the most crucial issues facing consumers. It has been showed that knowledge about data collection implications can have a negative impact on trust. Although some users claim that they are concerned about privacy while using apps, their actions do not support their claim. The seeming inconsistency between professed privacy concerns and risky behavior resulting from the use of smartphone apps may be more a consequence of ignorance rather than irrationality. This study is conducted to find out whether users are aware of the privacy issues and whether that awareness would influence their future usage behavioral patterns regarding download and use of apps. The study was conducted via a three phase survey. In the first phase, the survey was used to gauge smartphone users' privacy awareness and attitudes. A simple explanation of privacy implications of their actions was provided in the second phase and in the third phase, the users' attitudes were measured again. The survey results were used to test hypotheses to find out whether educating users about privacy implications of their smartphone apps download and use affect their subsequent usage. We posit that if the app users were made aware of the implication of policies regarding the collection of their personal information, their willingness to share that information would be negatively affected as manifested by an increase in their level of privacy concern and a reduction in their preferences to download and use of apps.

REVIEW of LITERATURE

The smartphones of today are more than just a calling device. The smartphone is also a video/voice recorder, camera, GPS, clock, gaming device, organizer, movie and music player, weather tracker, web browser, a gateway to access social media etc. The evolution of the mobile device led it to become a "social object present in every aspect of a user's life" (Srivastava, 2005). Since users carry their cellphones with them everywhere they go, they are always available on a 24×7 basis "Mobile phones allow users to construct their own 'at-home' environment, regardless of where they find themselves in physical space" (Srivastava, 2005). Storing almost all of our personal information such as phone numbers, photos, passwords, emails, notes etc. permanently in our handsets threatens privacy in case of theft, loss, or unauthorized access of the device.

Privacy

Privacy is concerned with control over individual's data (Shilton, 2009). Control over what data is captured, the accuracy of data, sharing of data, and duration of data retention. The data that has been captured can be used to process a person's likes, dislikes, habits, routines etc. (Shilton, 2009). Information privacy became a concern with the evolution of the internet and its wide use by people to go about their daily activities. This resulted in a flood of new data about individuals. This new form of online data gave rise to new concerns regarding the gathering and use of personal information. Table 1 tracks the evolution of information privacy concept following the evolution of IT.

Period	Characteristics
Privacy Baseline 1945-1960	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection.
First Era of Contemporary Privacy Development 1961-1979	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides of the new technologies (Brenton 1964), formulation of the Fair Information Practices (FIP) Framework and establishing government regulatory mechanisms established such as the Privacy Act of 1974.
Second Era of Privacy Development 1980-1989	Rise of computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national data protection laws for both the private and public sectors.
Third Era of Privacy Development 1990-present	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.

Table 1 – The Evolution of Information Privacy Concept Following the Evolution of IT (Smith, Dinev, & Xu, 2011)

Smith et al mentioned the following constructs which affect the privacy concerns: Privacy experiences, Privacy awareness, Personality differences, Demographic differences, and Culture. According to research conducted by Smith et al, it was found that individuals who have been targets of information exploitation are more inclined to protect and safeguard their information. Research suggests that the more users are aware, the more they start thinking about their privacy. Personality differences have also been found to play a major role in privacy concerns.

Privacy concerns using smartphones

A report by Forrester states that there will be one billion smartphone users by the year 2016 (Chen, 2012). According to an article in PC world, smartphone compromise user privacy through mobile applications. This includes tracing web habits, accessing contact list, making phone calls without user knowledge, tracking location, and automatically sending information (Preston Gralla, 2011). According to an article posted in ACLU website by Jay Stanley, he mentioned that "When you combine someone's personal information with vast external data sets, you create new facts about that person (such as the fact that they're pregnant, or are showing early signs of Parkinson's disease, etc.) and when it comes to such facts, a person a) might not want the data owner to know b) might not want anyone to know c) might not even know themselves. The fact is, humans like to control what other people do and do not know about them – that's the core of what privacy is, and data mining threatens to violate that principle" (Stanley, 2012). Another potential risk associated with big data is that data mining companies performing risk analysis for banking and insurance companies which for instance may sometimes " lower a customer's credit limit based on the repayment history of the other customers of stores where a person shops. Such "behavioral scoring" is a form of economic guilt-by-association based on making statistical inferences about a person that go far beyond anything that person can control or be aware of" (Stanley, 2012).

Information that smartphone applications gather

According to a research conducted by Intel, Penn State University, and Duke University, 15 out of 30 Android apps analyzed and sent information to remote servers without user knowledge. Twenty percent of the apps allowed third parties to access private information and 5% of the apps made phone calls without user intervention (Preston Gralla, 2011). According to the Wall Street Journal, 56 out of 101 apps examined transmitted unique user information without user's consent. Here is the list of information that the ten highest ranked applications (based on iTunes and Google store websites) gather while downloading those applications:

- **Network communication:** Allows the app to create network sockets and use custom network protocols.
- **Storage**: Allows the app to write to the USB storage and to write to the SD card.
- **Phone calls**: Allows the app to access the phone features of the device, to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.
- **Location-based Data**: Allows the app to get the approximate location and to get precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi.
- **System tools**: Allows the app to prevent the phone from going to sleep, to modify the sync settings for an account.
- **Personal information**: Allows the app to read and modify users' contacts.
- **Hardware controls:** Allows the app to take pictures and videos with the camera.
- **Accounts**: Allows the app to use the account authenticator capabilities of the Account Manager, including creating accounts and getting and setting their passwords, and to perform operations like adding and removing accounts, and deleting their password.
- **Messages**: Allows the app to read SMS messages stored on phone or SIM card.

Although there are advantages to participatory sensing, there are many hidden disadvantages as well. Participatory sensing allows gathering and sharing of information among people/communities; the information that is being shared is also inadvertently being tracked by enabling parties that relay the information such as the network operator and service provider. The information gathered might also be shared with third party stakeholders without the knowledge and consent of the participants. Over a period of time, a large amount of data is gathered and stored about each participant, which may be used to generate individual profiles to track user habits and understand individual patterns. It is imperative that the confidentiality and integrity of the data gathered is maintained.

Informed Consent

The major privacy concern with the gathering of user information is targeted mobile advertising. The information gathered, on its own does not amount to much, but when combined with location awareness and amount of personalized data gathered over a period of time results in the generation of precise individual patterns which can be used to send specific mobile ads to users. These unsolicited ads are construed as invasion of privacy by a majority of people across all demographics and are referred to as PUSH Advertising. PULL Advertising on the other hand, is advertisement that is generated upon user's "request on a one-time basis (e.g. a weather forecast)". However, mobile ads which are relevant to consumers are not considered to be spams. Most people are unaware that their smartphones are gathering their personal and location based information without their consent. Knowledge and informed consent affects users' decision to participate in sharing their personal information, their level of trust, and their decision regarding whether or not they want to receive an advertisement. Informed consent combined with a legal framework can provide consumer with information regarding their data and how it affects their privacy. According to Evelyne Beatrix Cleff "A combination of a legal framework, privacy-enhancing technologies, and consumer education may be important components of protecting consumer privacy." (Cleff, 2007) In order to make an informed decision, the user must be provided with all the relevant information and its impact on his/her privacy. The information should be such that it is easily understandable by a layman.

Effect of awareness on privacy concerns

Despite online privacy becoming a very hot topic over the past several years with an abundance of information easily available about its impact, a vast majority of netizens are still ignorant about online privacy, how it impacts them, and what remedial actions they can take to mitigate their exposure.

Research shows that people who are aware of the impact of privacy tend to be more cautious about sharing information and take steps to limit their exposure. Olivero and Lunt found that "an increase in privacy risk awareness reduces the level of trust and increases the demand for control over information use". (Olivero & Lunt, 2003) (Sheehan & Hoy, 1999). They will take steps to ensure that their privacy is protected. On the other hand, there are a lot of people who even though they are made aware of privacy issues and they claim that they will take steps to address their privacy concerns; their actions rarely reflect their concerns (Joinson et al., 2010).

Effect of awareness on privacy concerns based on age

The use of smartphones among younger people is higher, since they adapt to technology faster. Smartphone usage among the younger generation is so extensive that the device has almost become an extension of their body. Smartphone usage is changing the communication patterns of young people. As Srivastava mentions "Many teenagers don't recognize the difference between speaking on their mobile phone and meeting face to face." (Srivastava, 2005) Parents and teachers are also adapting to the way they communicate with the younger generation. For instance parents are increasingly using smartphones to keep track of their children.

The popularity of mobile applications among the younger demographic has led to retail and marketing companies to connect with their consumers through their own applications which keep the users updated about the latest products and offer them loyalty discounts or listen to music. They can keep in touch with their friends on social media by downloading social media apps (twitter, FB, foursquare) to their phones. Since a young person will be more willing and faster in adopting and using technology, he/she would be less concerned about privacy issues and sharing information with others compared to an older person who will be more circumspect in adopting technology and sharing information. The purpose of using mobile applications varies among various age groups for example people below 20 use mobile apps more for entertainment, games, and social networking, whereas, people above 30 might be using more of business, medical, and finance apps.

Effect of awareness on privacy concerns based on gender

It has been observed that the usage of smartphone varies across gender. In most countries women are higher users of smartphone as compared to men especially for talking and texting. For working mothers the smartphone has come as a boon as it helps them in balancing their family, social, and work lives (Srivastava, 2005). Smartphones are also allowing women to make better lifestyle choices. In 2001, NTT DoCoMo of Japan launched the iLady app, which acted as ovulation monitors. Also, in the UK, smartphones are being used to provide access to morning-after-pills and to impart sex education to female teenagers. Males and females have different patterns of using mobile apps.

For example males are more interested in sports and news applications. On the other hand females are more interested in social networking apps.

METHODOLOGY

To analyze the behavior of users on whether the users are concerned about privacy, a survey was conducted. The survey had questions in 5 different areas such as basic user information, demographic information, smartphone usage, testing user awareness, and privacy concerns. The demographic questions were used to gather information about the respondent age, education level, and gender. To measure the privacy concerns of users in the survey we asked the same question about downloading 13 different categories of mobile application in two different ways. First we asked them the following question: "What categories of apps did you download/use most often? Please check all that apply". After that we asked them "Knowing that these details are collected, which of the following apps would you still download / use in the future? Check all that apply". Based on the answers of the respondents to this awareness treatment, the paired sample t-test was applied to analyze the data.

Data Collection

A survey was designed with 32 questions asking users for their details such as age, location, education level, and also asking users about their privacy awareness and the steps they would take if they knew that their privacy was being affected. The survey link was sent to users through email and Facebook. There were about 250 responses out of which 187 qualified for analysis purposes, resulting in %75 response rates.

Data Analysis

Several different analytical techniques were used to analyze the data. Simple T-tests were used to test between-group differences in Privacy Concern. Z-tests of proportion were used to test the hypotheses of the study. ANOVA was used to test for differences between pre-test and post-test scores for privacy concern and for interaction effects. The average results were used to measure the pattern of downloading the apps before and after users were made aware of the privacy issues involved.

RESULTS

Demographics

From the survey it was determined that 43% of respondent use computers as their primary source of accessing the internet for more than 4 hours a day while 35% of respondents use computers all day every day. On the other hand, 29% of respondents use tablets and smartphones as their primary source of accessing the internet for more than 4 hours a day and 40% of respondents use them all day every day. According to the results of the survey, 69% of respondents have been using smartphones for less than 2 years and 31% have been using their smartphones for three years and more. In analyzing our sample, we found out that most of the respondents use internet the most at work, home, and while on the road. Using internet at home topped the survey with 182 responses, followed by internet usage at work with 112 responses and next was internet usage while on the road with 107 responses.

In analyzing the smartphone usage purpose, calling and texting was the number one reason given by users for using smartphones at 174 out of 187. Accessing the internet came in at number two with 173 responses. Personal and business email usage came in at number three with 138 responses. Games/apps came in number four with 133 followed by GPS usage at 129 responses.

Out of 187 respondents 183 people have downloaded free applications and 75 people have paid to download apps. Our sample was split into three categories- those who opted out, those who did not opt out, and those who were not sure. Results indicate that 44% of users claimed that they opted out from downloading applications due to privacy concerns, 33% did not opt out, and 23% of respondents were unsure.

Age

We divided our sample into three different age groups to determine the impact of age on smartphone applications privacy concerns. The age groups were below 20, between 21 and 30, and above 31. People below 20 years of age accounted for roughly 43% of the respondents. People between 20 – 30 years of age accounted for 44% of the respondents and people above 31 accounted for 13% of the age group.

Level of Education

Respondents were divided into three groups based on their level of education. The first group consisted of high school diploma holders at 41%. The second group consisted of undergraduate and college degree holders at 37%. The final group consisted of master degree holders and above at 22%.

Gender

Gender was used as a demographic question in order to determine if it affected the range of downloading applications. Females accounted for 63% of respondents and males for 37%.

DISCUSSIONS

The main focus of this research can be found in table 2, which provides an overview of the results. The most downloadable types of mobile applications on iTunes are classified under the following three categories: Entertainment, Social Networking, and Navigation (Listed in table 2). These findings have implication for consumers, application stores, and policy makers. On the consumer side, it is essential to protect one's own privacy. Our results indicate that consumers may not fully understand online data collection and the related privacy issues. Therefore, consumer education is important. Those consumers who are concerned about online privacy should be meticulous in reading privacy policies in order to establish what information is collected. If a consumer is uncomfortable with the information that will be collected and/or how that information will be employed, they have the opportunity to visit another site or eschew the risky transaction. Users should also be aware of the technology available to help protect privacy. In addition, consumers must become aware that an inherent tradeoff exists between the convenience of mass customization and privacy risks online. Consumers must weigh the potential benefits versus the potential risks and make an informed choice regarding preferences for downloading the application.

Applications	Pre-Test		Post-Test		Sig.
	Avg.	SD	Avg.	SD	
Entertainment (e.g., Music, Books, Movies)	.38	.81	.27	.78	.000
Social Networking (e.g., Face book, Twitter)	.46	.82	.34	.80	.000
Navigation (e.g., Google Maps, GPS)	.31	.79	.20	.76	.000

Table 2 – Pre-Test and Post-Test results

CONCLUSION

These finding also have implications for app stores. Our findings showed increased levels of privacy concern as consumers were made aware of information gathering technology. Olivero and Lunt found that an increase in privacy risk awareness reduces the level of trust and increases the demand for control over information use (Olivero & Lunt, 2003). Policy makers will also have to deal with the issue of on-line privacy in the coming years. According to the Center for Democracy & Technology, there were at least twelve bills introduced in the 108th US congress related to privacy and the internet (Privacy Legislation Affecting the Internet: 108th Congress, 2004). We find the number of people that claim to be concerned about privacy is increasing (Ribak & Turow, 2003); yet people continue to perform activities that are risky in terms of privacy. Some researchers and interest groups argue for self-regulation on the grounds that consumers are free to make a choice with respect to participating in on-line information exchange (Ribak & Turow, 2003). Their argument is bolstered by the findings of Westin who submits that the majority of internet consumers are "privacy pragmatists" (Westin, 2003). His description of these users suggests that they make informed cost-benefit decisions regarding internet privacy risks. Our findings dispute this assertion. The results of this study suggest that a significant number of people do not understand the technology and risks associated with surreptitious information collection on the internet. If people do not understand the fast changing technology, regulations, and privacy laws that govern internet privacy, it is unrealistic to expect them to make an informed choice. Our findings support the need for further regulation and increased and internet users education concerning surreptitious data collection using apps.

REFERENCES

1. Privacy Legislation Affecting the Internet: 108th Congress. (2004). Retrieved from Center for Democracy & Privacy: https://www.cdt.org/legislation/108th/privacy
2. Bansal, G., Zahedi, F., & Gefen, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, PrivacyConcern and Trust in Disclosing Health Information Online. Decision Support Systems, 138-150.
3. Chen, B. X. (2012, February 14). Get Ready for 1 Billion Smartphones by 2016, Forrester Says. Retrieved July 3, 2012, from nytimes.com: http://bits.blogs.nytimes.com/2012/02/13/get-ready-for-1-billion-smartphones-by-2016-forrester-says/
4. Cleff, E. B. (2007). Privacy Issues in Mobile Advertising. INTERNATIONAL REVIEW OF LAW COMPUTERS, 225-236.
5. Combe, C., Colley, A., Hargreaves, D. J., & Dorn, L. (1997). The effects of age, gender and computer experience upon computer attitudes. Talor and Francis.
6. Culnan, M. J. (1995). Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing. Journal of Interactive Marketing, 10-19.
7. Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. (2010). Privacy, Trust, and Self-Disclosure Online. Taylor & Francis, 1-24.
8. Olivero, N., & Lunt, P. (2003). Privacy versus willingness to disclose in E-commerce exchanges: the effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology.
9. Pavlou, P. A. (2011). state of the information privacy literature: where are we now and where should we go? MISQ.
10. Preston Gralla, A. S. (2011, June 7). Smartphone apps: Is your privacy protected? Retrieved from Computerworld:
11. Ribak, R., & Turow, J. (2003). Internet Power and Social Context. Journal of Broadcasting & Electronic Media, 328-340.
12. Sheehan, K. B., & Hoy, M. G. (1999). Using E-Mail To Survey Internet Users in the United States: Methodology and Assessment. Journal of Computer-Mediated Communication.
13. Shilton, K. (2009). Four Billion Little Brothers? Privacy, mobile phones, and ubiquitous data collection. Communications of the ACM, 5.
14. Smith, A. (2011, June 11). Smartphone Adoption and Usage. Retrieved May 2, 2012, from Pew internet reports: http://pewinternet.org/Reports/2011/Smartphones.aspx
15. Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly.
16. Srivastava, L. (2005). Mobile phones and the evolution of social behaviour. Behaviour & Information Technology, 111-129.
17. Stanley, J. (2012, April 25). Eight Problems with "Big Data". Retrieved July 3, 2012, from ACLU: http://www.aclu.org/blog/technology-and-liberty/eight-problems-big-data
18. Westin, A. (2003). Consumers Show Increased Willingness to Accept Biometric Identifiers. Credit Union Executive Center.
19.